
EXHIBIT A

SUBJECT JD-ZACH, MALE WHITE, APPROX 25-35 YEARS OLD, APPROX 220 LBS, APPROX 5'10 HGT, HEAVY BUILD, LIGHT COMPLEXION, BROWN EYES, BALD HEAD, BEARD, TATTOO RIGHT ARM "GREEN STAR", TATTOO LEFT LEG BEACH SCENE WITH NAME "TOM"

AT VARIOUS TIMES AND DATES FROM SPRING 2019 – JANUARY 16, 2020, I UC 0394 DID ENGAGE IN CONVERSATION WITH SUBJECT JD-ZACH WHILE CONDUCTING A MAJOR CASE VICE OPERATION REGARDING PEDOPHILIA. DURING THE COURSE OF CONVERSATION, I ASSUMED THE IDENTITY OF A 14-YEAR-OLD BOY. DETAILS ARE AS FOLLOWS:

ON JANUARY 16TH, 2020 AT APPROX 1500 HRS JD-ZACH DID CONTACT ME VIA SNAPCHAT ACCOUNT HANDLE "ZACHS6015". SUBJECT ASKED ME IF HE SHOULD BRING CONDOMS AND WE AGREED TO MEET AT A LOCATION. I MAINTAINED CONTACT WITH SUBJECT VIA CELL PHONE. I WALKED INTO THE STATEN ISLAND FERRY TERMINAL LOCATED AT 4 WHITEHALL ST, NEW YORK, NY, AND INFORMED SUBJECT THAT I WAS INSIDE. AT APPROX 1638 HRS SUBJECT STATED THAT HE WOULD ARRIVE AT AGREED LOCATION IN ABOUT 30 MINS. AT APPROX 1725 HRS SUBJECT ASKED "YOU INSIDE OR OUTSIDE". AT APPROX 1728 HRS SUBJECT WAS APPREHENDED BY FIELD TEAM.

THE SUBJECT WAS LATER IDENTIFIED AS SCHEININ, FREDERICK, DOB [REDACTED], ARREST # M20602117

TAC PLAN CASE # 2020-0004

SI KITE # 2019-108-8

A/O: DET ADASZEWSKI

GHOST: DET WILLIAM PEREZ

WEATHER: CLEAR, COLD NIGHT

LIGHTING: LIT

EXHIBIT B



U.S. Department of Justice

*United States Attorney
Southern District of New York*

*The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007*

May 17, 2021

BY EMAIL

Tamara Giwa, Esq.
Federal Defenders of New York
52 Duane Street
New York, NY 10007

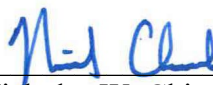
Re: *United States v. Frederick L. Scheinin*, 20 Cr. 133 (LGS)

Dear Ms. Giwa:

The Government writes to inform you that it does not possess, and is unable to obtain, certain communications that the Government understands were exchanged between the defendant and an undercover law enforcement agent ("UC-1"). The Government understands that at some time before October 26, 2019, the defendant initiated contact with a Grindr account operated by UC-1. The Government understands that this communication was brief. The defendant's initial contact contained a photograph of an erect penis that appeared to have ejaculated on a table or furniture. In UC-1's response to the defendant, UC-1 stated, in sum and substance, that UC-1 was 14 years of age. The defendant continued to communicate with UC-1. Following this brief exchange, Grindr deactivated UC-1's Grindr account due to a violation of the terms of service and, as a result, UC-1 lost these initial communications with the defendant. UC-1 created a new account, and on or about October 26, 2019, the defendant reinitiated contact with UC-1 over Grindr.

Very truly yours,

AUDREY STRAUSS
United States Attorney

by: 

Nicholas W. Chiuchiolo / Daniel G. Nessim
Assistant United States Attorneys
(212) 637-1247 / 2486

EXHIBIT C



U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

May 26, 2021

BY EMAIL

Tamara Giwa, Esq.
Sylvia Levine, Esq.
Federal Defenders of New York
52 Duane Street
New York, NY 10007

Re: *United States v. Frederick L. Scheinin*, 20 Cr. 133 (JSR)

Dear Counsel:

The Government writes in response to your letter dated May 21, 2021. The undersigned Assistant United States Attorneys are available to discuss these issues in more detail.

1. The Government is not aware of the exact date of the first communication between the defendant and UC-1¹ but understands, based on conversations with UC-1, that the defendant first contacted UC-1 on Grindr approximately one or two months prior to October 26, 2019.

2. UC-1 recalls that there were approximately a dozen messages with the defendant in this pre-October 26 interaction and that this exchange took place over the course of several days.

3. UC-1 recalls that, in the conversation that occurred prior to October 26, 2019, the defendant sent several sexually explicit photographs, including a photograph of an erect penis that appeared to have ejaculated on a table or furniture. UC-1 later identified this photograph among the photographs that were extracted from the defendant's black Apple iPhone, assigned call number [REDACTED], with IMEI number [REDACTED]. UC-1 does not recall whether UC-1 sent photos to the defendant prior to October 26, 2019, but it is not UC-1's typical practice to send photos to a subject during initial communications.

4. The Government understands that Grindr deactivated UC-1's account because of a violation of Grindr's terms of service. Grindr did not inform UC-1 of the specific term of service that had been violated. At or around the time of the deactivation of UC-1's Grindr account, UC-1 had been communicating with multiple individuals, including the defendant, and represented to all of those individuals that UC-1 was a minor. Grindr prohibits individuals under the age of eighteen from using Grindr services.

¹ As used herein, UC-1 has the same meaning ascribed to it in the Complaint. (See Compl. ¶ 7(a) n.2.)

5. UC-1 does not recall the date that UC-1's Grindr account was deactivated. Grindr did not send UC-1 a formal notice of deactivation. Rather, when UC-1 attempted to log in, the Grindr application informed UC-1 that the account had been deactivated due to a violation of the terms of service.

6. UC-1 believes that a new account was created on or after September 20, 2019.

7. UC-1 lost access to UC-1's Grindr communications when Grindr suspended the account. Accordingly, UC-1 discovered that the communications made before October 26, 2019 were not preserved on or about the same date that UC-1's Grindr account was deactivated.

8. The United States Attorney's Office (the "USAO") was aware of communications between UC-1 and the defendant made prior to October 26, 2019—*see* Compl. ¶ 6—and learned during the investigation that UC-1 had lost access to those communications.

9. The USAO opened its investigation into the defendant on or about November 19, 2019. That same day, the Government directed Grindr to preserve any and all information associated with Grindr accounts registered by email addresses believed to be associated with the defendant. A copy of the November 19, 2019 preservation notice is annexed hereto as Exhibit A. On November 20, 2019, the Government directed Grindr to preserve any and all information associated with Grindr accounts registered by email addresses used by UC-1. A copy of the November 20, 2019 preservation notice is annexed hereto as Exhibit B.

10. The Government has investigated your claim that communications are "missing" and responds to it as follows:

- a. For the communications you assert are missing or incomplete in communications taking place on November 8, 2019; November 11, 2019; November 14, 2019; December 11, 2019; the forty-minute gap referenced on December 19, 2019; the assertion that two days of conversation are missing prior to January 2, 2020; January 9, 2020; and January 14, 2020, the Government is not aware of any additional communications on these dates and is not aware of the basis for the contention that these conversations are incomplete. For November 8, 2019, for example, the discovery production includes messages sent and received during the timeframe your letter asserts items are missing (available in discovery at USAO_001109-001113);
- b. The December 4, 2019 text message is available in discovery at USAO_000721;
- c. For the asserted possible missing information in communications taking place on November 15, 2019; November 18, 2019; December 9, 2019; and January 2, 2019, the Government agrees that a portion of these communications may lack context. The Government is not aware of the basis for that missing context and understands that all screenshots of the communications on these days have been produced;

- d. With regard to the images you reference that were sent on December 19, 2019; December 20, 2019; and January 7, 2020, some of these photographs were produced in the initial discovery production as “##Photos Sent by CS.” We have also obtained additional images that were saved on UC-1’s phone’s camera roll on the relevant dates and at the relevant times. Some of these images were the ones sent by UC-1 to the defendant on December 19, 2019 and December 20, 2019. We are producing (or reproducing) to you as discovery today these photographs (and one video) with the corresponding “detail” page that provides information concerning the creation date and time, among other things; and
- e. The January 15, 2020 images depicting a building’s exterior were taken to document the view that UC-1 showed the defendant in a January 15, 2020 conversation produced as USAO_000877.

11. As described in the preceding response, the “detail” information for the photographs produced in the ##Photos Sent by CS folder, are being produced to you in discovery today.

12. The Government disputes the defendant’s assertion that the “discovery production does not include any photographs or video depicting UC-1’s face.” UC-1 sent the defendant a photo depicting UC-1’s face on or about November 6, 2019 at 9:33 p.m. This photograph bears bates numbers USAO_000722 and USAO_000725 (which were designated as “Sensitive Material” under the protective order) and was produced to the defense on or about February 28, 2020.

13. The Government is unaware of video communications between UC-1 and the defendant that have not been produced to the defense.

14. On the defendant’s behalf, the Government has requested all records that the Queens County District Attorney’s Office obtained pursuant to subpoenas. As for the defendant’s request for copies of “all subpoenas,” please provide a basis and legal authority for this request.

15. Attached as Exhibit C are additional preservation requests.

Very truly yours,

AUDREY STRAUSS
United States Attorney

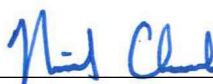
by: 
Nicholas W. Chiuchiolo / Daniel Nessim
Assistant United States Attorneys
(212) 637-1247 / 2486

EXHIBIT D

20 MAG 14 65

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the iCloud Account
[REDACTED]@yahoo.com Maintained at
Premises Controlled by Apple, Inc., the
Snapchat Account [REDACTED]
Maintained at Premises Controlled by
Snap Inc., and the Grindr Account
[REDACTED]@yahoo.com Maintained at
Premises Controlled by Grindr LLC,
USAO Reference No. 2019R00731

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

**Agent Affidavit in Support of Application for a Search Warrant
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

PHILIP ADASZEWSKI, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Detective with the New York City Police Department ("NYPD"), currently assigned to the Vice Major Case Unit. I am assigned to a group charged with enforcing laws prohibiting child pornography and other forms of child exploitation. As such, I have worked on numerous investigations and prosecutions involving minor victims and the adults who victimize these children. During the course of these investigations, I have participated in the execution of search warrants involving electronic evidence, including social media accounts.

B. The Provider, the Subject Accounts and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for content and other information associated with:

a. The iCloud account [REDACTED]@yahoo.com ("Subject Account-1"), maintained and controlled by Apple, Inc. ("Apple"), headquartered at One Apple Park Way, M/S 169-5CLP Cupertino, CA 95014-2084.

b. The Snapchat Account [REDACTED] ("Subject Account-2"), maintained and controlled by Snap, Inc. ("Snap"), headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405.

c. The Grindr Account [REDACTED]@yahoo.com ("Subject Account-3", together with Subject Account-1 and Subject Account-2, the "Subject Accounts"), maintained and controlled by Grindr LLC ("Grindr"), located in Los Angeles, California.

3. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

4. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) (attempted production of child pornography), 2422(b) (attempted coercion and enticement of a minor to engage in illegal sexual activity), 2252A(a)(5)(B) (attempted possession of child pornography), and 2252A(a)(2)(B) (attempted receipt of child pornography) (collectively, the "Subject Offenses").

C. Services and Records of the Provider

5. Based on my training, experience, and participation in this investigation, I have learned the following about Apple:

a. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

b. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

i. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

ii. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

iii. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

iv. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and

passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

v. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

vi. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

vii. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

viii. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

c. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

d. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a

third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

e. Apple captures information associated with the creation and use of an Apple ID.

During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

f. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service,

including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

g. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may

maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

h. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service

(“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud Drive. Some of this data is stored on Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

i. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

j. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

6. Based on my training, experience, and participation in this investigation, I have learned the following about Snapchat, an online communication service offered by Snap to the public:

a. Snapchat is a multimedia messaging application that offers its users the ability to communicate with each other through text messaging and real-time video chat. Users can create multimedia messages—such as photographs or short videos, which can be edited to include filters, effects, drawings, and captions—and send such messages to other Snapchat users.

b. Snapchat messages can be viewed by the recipient for a user-specified period of timer (typically between one to ten seconds) before they become inaccessible.

c. Snapchat also allows its users the ability to communicate with each other through real-time video chats.

d. Depending on a user's account features and settings, Snapchat sometimes maintains records of communications sent or received by its users. In addition, Snapchat sometimes maintains geolocation information associated with users.

e. Upon creating a Snapchat account, a Snapchat user can create a unique Snapchat username and account password or key. This information is collected and maintained by Snapchat.

7. Based on my training, experience, and participation in this investigation, I have learned the following about Grindr:

a. Grindr is a social networking application that allows its users to communicate with other Grindr users, including by sending and receiving text, photo, video, and multimedia messaging. Depending on a user's account features and settings, Grindr sometimes maintains records of communications sent between its users.

b. Grindr users can create unique profiles, which Grindr maintains.

c. Grindr operates on iOS and Android operating systems.

d. Grindr also maintains geolocation information for some users, which allows users to locate other users who are nearby.

e. Upon creating a Grindr account, a Grindr user can create a unique Grindr username and account password or key. This information is collected and maintained by Grindr.

D. Jurisdiction and Authority to Issue Warrant

8. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the

Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

9. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

10. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

11. The NYPD and the Department of Justice, Office of Inspector General (the “DOJ-OIG”, together, the “Investigating Agencies”) have been investigating FREDERICK SCHEININ for violations of the Subject Offenses.¹ In particular, since approximately October 2019, SCHEININ had been communicating with an undercover law enforcement officer (“UC-1”)—using, among other means, Subject Account-2 and Subject Account-3. During communications with SCHEININ, UC-1 posed as a fourteen-year-old boy. As set forth in greater detail below,

¹ DOJ-OIG assisted in this investigation because, up until the time of his arrest, FREDERICK SCHEININ was a diversion investigator in Drug Enforcement Administration’s New York Field Office.

SCHEININ attempted to induce UC-1 to engage in sexual activity with SCHEININ and to transmit sexually explicit images and videos of UC-1.

12. On January 16, 2020, the Investigating Agencies arrested FREDERICK SCHEININ in Manhattan for violations of the Subject Offenses.

13. On January 17, 2020, the United States Attorney's Office for the Southern District of New York filed a complaint (the "Complaint" or "Compl.") against FREDERICK SCHEININ, which was signed that same day by the Honorable Katharine H. Parker, United States Magistrate Judge for the Southern District of New York. The Complaint is attached hereto as **Exhibit 1** and incorporated by reference.

14. Based on the information set forth in the Complaint, I respectfully submit that there is probable cause to believe that FREDERICK SCHEININ has been engaged in the Subject Offenses.

B. Probable Cause Regarding the Subject Accounts

15. Based on my review of documents, evidence, and conversations with law enforcement officers as well based on my training and experience, I have learned the following, among other things:

Subject Account-3

a. In an effort to detect and apprehend perpetrators of child exploitation offenses, law enforcement officers working with the NYPD have occasionally operated an undercover account (the "UC Account") on Grindr, a popular social networking dating application. Based on my training and experience, I am aware that Grindr's terms of service prohibit children below the age of eighteen from creating or using accounts on their service. However, based on my participation in this investigation and my training and experience, I am aware that minors frequently use Grindr to communicate with and meet other individuals. Due to Grindr's terms of service, the profile for the UC Account listed the user's age as eighteen, but the law enforcement officers who operated

the UC Account typically told individuals who communicated with the UC Account that the operator of the UC Account was fourteen years old.

b. Beginning in or around October 2019, an individual believed to be FREDERICK SCHEININ, began communicating with the UC Account using Subject Account-3. In particular, Subject Account-3 transmitted sexually explicit images of, among other things, an erect penis.

c. The law enforcement officers operating the UC Account told SCHEININ, in substance and in part, that the user of the UC Account was fourteen years old. Notwithstanding, SCHEININ continued to use Subject Account-3 to communicate with UC-1, whom SCHEININ believed to be a minor.

d. On or about October 26, 2019, SCHEININ used Subject Account-3 to send his cellphone number, [REDACTED] (the "Scheinin Phone Number"), to the UC Account. Sometime after, SCHEININ used the Scheinin Phone Number to communicate directly with UC-1, including through applications like Google Voice and Snapchat.

Subject Account-2

e. On or about November 7, 2019, using Google Voice, SCHEININ and UC-1 discussed communicating through Snapchat, which has a real time video chat function. During this November 7 Google Voice text exchange, SCHEININ sent UC-1 his Snapchat username: [REDACTED] i.e., Subject Account-2.

f. On or about November 8, 2019, SCHEININ and UC-1 communicated in real time using Snapchat's video chat. During this communication and all other video communications with SCHEININ, UC-1's appearance was partially disguised to be consistent with that of a fourteen year-old boy. During this November 8 communication, UC-1 asked SCHEININ, "so you like don't care that I'm younger?" SCHEININ responded, "No, it's cool. As long as you're cool with

it.” Approximately one minute later, SCHEININ asked UC-1, “have you ever like done anything on [Snapchat] before, you know, like, jerked off with someone or anything like that?” SCHEININ then stated, in substance and in part, that he had masturbated on Snapchat and that it was “all right” but that “it’s better in person.

g. Over the two months that followed, UC-1 and SCHEININ regularly communicated, using Subject Account-2. During some of these communications, SCHEININ attempted to induce UC-1 to transmit live visual depictions of UC-1 penis. For example, or about January 7, 2020, SCHEININ and UC-1 communicated in real time using Snapchat’s video chat feature. During this conversation, SCHEININ used Subject Account-2 to (repeatedly) requested that UC-1 take sexually explicit photos of UC-1’s penis and send the photos to SCHEININ through Subject Account-2 and/or that UC-1 show UC-1’s penis to SCHEININ using Snapchat’s video chat. In response to SCHEININ’s requests, UC-1 stated, “I kinda want to,” and SCHEININ responded, “I think you should. Just really quick.” UC-1 and SCHEININ then engaged in the following colloquy, in substance and in part:

| | |
|-----------|--|
| UC-1: | Well, I’m not ready right now . . . because it’s soft. So I don’t know if you’d wanna see it soft. |
| SCHEININ: | Well, I’ll see it soft first and then see what happens.. |
| UC-1: | So you don’t care if it’s hard or soft? |
| SCHEININ: | I mean, I think I’d like to see it both ways and then I’ll see which way I like it better. |
| UC-1: | I don’t know yet. I have to feel more comfortable first. |
| SCHEININ: | All right. That’s cool. |
| UC-1: | I’m still nervous. |
| SCHEININ: | What are you nervous about? |
| UC-1: | I Don’t know. Because I haven’t met yet in person. Does that bother you? |
| SCHEININ: | No. But I still want to see it. |

h. SCHEININ also used Subject Account-2 to attempt to entice UC-1 to engage in sexual activity. During a January 15 video chat over Snapchat, UC-1 asked SCHEININ what they would do when they met in person, and SCHEININ stated, in sum and substance, “I don’t know; we’ll figure it out.” UC-1 responded, “but I like hearing about it.” SCHEININ then stated, in sum and substance, “No. Because you’re in public and shit.” UC-1 then asked, “you still want to fuck?” and SCHEININ responded, “yeah. . . . Are you sure you can handle it?”

Subject Account-1

i. From October 2019, up until the time of his arrest in January 2020, SCHEININ regularly used his cellphone—using various messaging applications, including Subject Account-2 and Subject Account-3—to communicate with UC-1 in furtherance of the Subject Offenses. At or about the time of his arrest on January 16, 2020, law enforcement seized two cellphones from the defendant: a personal Apple iPhone and an Apple iPhone that was issued by the Drug Enforcement Administration in SCHEININ’s capacity as a diversion investigator. Law enforcement subsequently obtained a search warrant to search both cellphones and, based on law enforcement agents’ review of the limited information that has been obtained thus far from SCHEININ’s personal cellphone, I am aware that SCHEININ maintained an Apple iCloud account with the username [REDACTED]@yahoo.com, *i.e.*, Subject Account-1.

j. Based on my review of records obtained from Apple pursuant to a grand jury subpoena, I am aware that Subject Account-1 is subscribed to in the name “Frederick Scheinin” and that content was regularly backed up to Subject Account-1. I am further aware based on my review of records obtained from Apple that Subject Account-1 was active during Investigating Agencies’ investigation into SCHEININ, including up until the day of the arrest on January 16, 2020.

k. Based on my training and experience, I have learned that iCloud retains copies of messages, photographs, videos, location history and documents, stored by users and copies of those items are maintained by Apple for extended periods of time unless deleted by the user. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation, including text, video, and multimedia communications between SCHEININ and UC-1 or other minors. In addition, based on my training and experience, I know that individuals who engage in the Subject Offenses, including the production of child pornography and the enticement of minors to engage in illegal sexual activity, commonly use computers and other electronic devices to, among other things, communicate with victims, communicate with other individuals who engage in similar unlawful activity, solicit child pornography from others, maintain and store libraries of child pornography for future exploitation. As a result, they often store data on their computers and other electronic storage devices, including external data storage devices, related to their illegal activity.

16. The Government submitted a preservation request for Subject Account-1 to Apple on or about January 27, 2020 (Apple reference number 20315681), a preservation request for Subject Account-2 to Snap on or about January 15, 2020 (Snap reference number 63982934), and a preservation request for Subject Account-3 to Grinder on or about November 19, 2019 (Grinder reference number 3442135).

17. Accordingly, and based on the foregoing, there is probable cause to believe that the Subject Accounts may contain evidence of the Subject Offenses, such as (i) evidence of communications between FREDERICK SCHEININ and UC-1 or other minors; (ii) evidence of visual depictions of child pornography; (iii) evidence of attempts to download or otherwise receive child pornography; (iv) evidence of SCHEININ's control and use of the Subject Accounts.

18. This application seeks content from the Subject Accounts during specified time frames relevant to the Subject Offenses: January 1, 2019 through January 16, 2020.

C. Evidence, Fruits and Instrumentalities

19. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

20. In particular, I believe the Subject Accounts are likely to contain the following information:

- a. The creation, content, and ownership of the Subject Accounts.
- b. The creation or ownership of the telephone number [REDACTED], which was used to communicate with UC-1 between in or about October 2019 and the present.
- c. Communications with UC-1 between October 2019 and the present.
- d. Evidence of other email accounts, social medial accounts, cloud storage accounts, or repositories of evidence concerning the Subject Offenses and passwords to access such accounts.
- e. Images or videos depicting child pornography.
- f. Evidence of attempts to download or otherwise receive child pornography or to visit websites on which child pornography is available between January 2019 and the present.
- g. Communications with individuals aimed at enticing or persuading a minor to engage in illegal sexual activity between January 2019 and the present.
- h. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment.
- i. Evidence reflecting registration of other online and social media accounts themselves potentially containing relevant evidence between January 2019 and the present.
- j. historical location data showing the user's movements;
- k. digital photographs and video relating to the Subject Offenses;

1. evidence of user attribution showing who used or owned the Subject Accounts at the time the records and items described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

III. Review of the Information Obtained Pursuant to the Warrant

21. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Providers, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 14 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

22. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique

words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

23. Although the defendant has already been arrested, the full scope of this ongoing criminal investigation is not publicly known. For example, the defendant may not be aware that the Government is investigating charges beyond those alleged in the indictment, such as possession of child pornography and receipt of child pornography unrelated to SCHEININ's communications with UC-1. As a result, premature public disclosure of this affidavit or the requested warrant would alert SCHEININ to the full scope of the criminal investigation, causing him, directly or indirectly, to destroy evidence (*see* 18 U.S.C. § 2705(b)(3)), flee from prosecution (*see* 18 U.S.C. § 2705(b)(2)), or otherwise seriously jeopardize the investigation (*see* 18 U.S.C. § 2705(b)(5)). This risk is heightened with respect to the Subject Accounts because these accounts can be deleted remotely.


24. Accordingly, there is reason to believe that, were the Providers to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Providers not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

25. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose

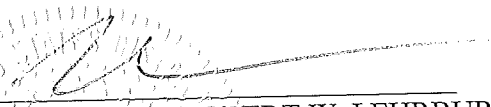
those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

26. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.


Detective Philip Adaszewski
NYPD

Sworn to before me this
10th day of February, 2020


HONORABLE ROBERT W. LEHRBURER
United States Magistrate Judge
Southern District of New York

